Single Sign-On Benefits and Challenges

Single Sign-On, or SSO, is a critical piece of effective security in your business. With a SSO service, users get access to multiple destinations of a network with a single login – one username and one password.

Streamlining the login process makes the workflow move smoother. Not only this, but it makes things safer because errors are reduced.

For example, let's say users generally access five applications during a work shift.

Without SSO, they're going through five login routines – which multiples the risk of mistakes. With more mistakes, more time is wasted. It's worth mentioning, though that while SSO does offer easier access, there is some risk involved.

How SSO Works

The SSO service provider authenticates a user for all applications they have the rights to. It doesn't require any more action when switching between any of the authorized apps.

The app server gets the user credentials from the dedicated SSO policy server, then checks the person against a known user directory.

SSO offers a variety of access methods, system configurations, and login processes available to choose from. As such, your organization can select the SSO system that works best for your specific needs.

Options do get fairly complex, so it's a good idea to have an IT professional or expert evaluate them before you choose the one you want to use.

SSO eliminates tasks and helps with user-account oversight and activity management. With it, however, comes a major security risk. If a hacker is able to gain control over user credentials, they can make it through every application that the user has access to. As such, password security is a big issue. It's also important to protect usernames, email, and promote careful browsing online.

Identity providers supply SSO capabilities. The entities and what they offer are not the same, so choosing the right one is an important decision.

You'll need to understand the difference between security assertion markup language (SAML), OAuth, and OpenID connect, for instance.

It's not one you should make without input from an expert. One of the main goals in choosing the right SSO provider is getting one that has the capability to serve a wide range of users.

However, it may be essential to add at least one additional authentication system to protect everyone within an organization.

Let's take a closer look at how it works on the front end for users, first without SSO – and then again with.

The Process Without SSO

1. The user hits a page on a website that checks to see if they are already logged in. If the user is, the authentication completes, and the system forwards the user to wherever they wanted to go in the first place.
2. If the user isn't already logged in, they are presented with a login screen.
3. The user enters their login credentials in the form, and the website checks the credentials against its database. The login is either approved

and the user is permitted access, or denied.
4. If the login is successful, the website issues a tracker. This is usually on the server, but in some instances may also be sent over to the user's computer as a token.
5. Now, whenever the user moves around the website, the system checks to make sure the tracker (and the authentication that goes with it) is current.

The Process With SSO

1. The user hits a page on a website – the SSO portal – that checks to see if they are already logged in. If they are, it takes the user to whatever they wanted in the first place.
2. If the user isn't already logged in, they are presented with a number of authentication service options with a third-party identity provider, such as Google, Facebook, or Amazon. The user picks the provider of their choice. For the sake of this example, let's say our user selects Google.
3. Google then checks to make sure the user is who they say they are (user authentication), then checks to make sure the website using the service is who it claims to be. The user is authenticated based on the Google password database. Then Google issues a token back to the website the user is attempting to login to.
4. The website gets the token, which verifies the user's identity. It now connects the user with the rest of the user's data – history, preferences, shopping cart, etc.

In a true SSO system, users can move around from one website to another with full access.

With a delegated system, Google returns a verification of identity along with a set of authorized uses. The website may be given access to a user's name and email address, but not location or age, for instance.

> *Single sign on solutions are popular with SaaS because it makes it easy for new users to sign up and use it.*

Benefits of Single Sign-On

- **Improved identity protection:** With SSO, companies can add two-factor authentication (2FA) and multifactor authentication (MFA), for better security. This ensures that all user access is authenticated by more than just the one login.

- **Reduces security risks for customers, vendors, and other partner organizations:** Connections between you and trusted third parties are always vulnerable and a point of risk. SSO can reduce the risk and improve cybersecurity.
- **Increases speed where you need it:** SSO means that users don't have to spend a lot of time with a signup and authorization process. Google (or another SSO option like Facebook or Amazon) has already done the verification and data collection, so new users can sign up and login as quickly as it takes to login to Google. There's no need to worry about how many password resets people go through before they can access the data they need. This is particularly helpful in health care, defense, and emergency services, for instance – as they are industries where speed is of the essence. When dealing with large numbers of departments and people needing fast and uninhibited access to the same applications, SSO may mean the difference between life and death.
- **Reduces IT help desk calls and workload:** When there are fewer people calling or emailing for help with lost passwords, the company saves money and improves security.
- **Simplifies identity and access management:** When personnel changes happen, SSO makes things easier on the IT department. There are fewer chances for mistakes. All it means is that employees who leave the organization surrender their login privileges.
- **Transparency:** Users know, at least in the case of delegated systems, what's being shared from one system to another If they aren't happy with the options, they can opt-out.
- **Convenience:** Users will only need to remember one set of login credentials. By connecting your platform to users' Google logins, you make sure that even occasional users always know how to login. It helps to reduce password fatigue, which makes it easier for users to come up

with more complex and thus more secure, passwords.

- **Security:** Users have peace of mind knowing that website and application owners don't have their passwords stored in plain text files somewhere, waiting to be shared on the dark web. Google remains the main trust point, which is a critical part of the user experience.

Challenges of SSO

- **You must enforce strong passwords:** If an SSO account is compromised, users with the same authentication can be at risk.
- **If SSO goes down, all access to connected sites stops:** That's why it's important to choose the right SSO system. Take your time and do your research.
- **If your identity provider goes down, so does your SSO:** If the provider is vulnerable, then you are, too. What's more, is that it is probably out of your control. Yet another reason to choose your provider with care.
- **If a hacker breaches an account, all linked systems become vulnerable:** This is a classic single failure point. Do what you can to address in the planning phase. High-quality SSO providers have top-of-the-line security measures to protect themselves and you – as their customers.
- **You may run into conflicts if you use SSO with social networking services:** If your workplace blocks social media, but gives Facebook as an option for SSO, this can create issues. That's why a lot of organizations opt to use Google as the main authenticating service.
- **SSO can take a bit longer to set up:** Every environment is unique. Added implementation steps may pop up unexpectedly, which can increase the length of time it takes to get things up and running. Linking the identity provider to the service provider, for instance, may take a bit longer than you realized.
- **Risky for computers with multiple users:** If you're in an industry where multiple people use the same computer, such as a call center, for instance, it can be a bit of a hassle. Think about what happens when one user is logged in and another one needs to use the computer.
- **You may need to rely on reduced single sign on (RSO) if you need**

to accommodate multiple access levels: If different users require different access levels, you may need to add additional authentication servers to accommodate the access control.
- **Some SSO-linked sites may supply data to third parties:** This is something you need to pay close attention to – especially if you are in a highly regulated industry.

The challenges of SSO are definitely worth concerning yourself about, but none of them are impossible. The benefits of SSO are much stronger than the challenges with SSO solutions.

But, to make the most of your effort, it's important to have expert guidance along the way. This allows you to maximize the benefits while reducing the risks.

What's your goal today?

1. Use PLANERGY to manage purchasing and accounts payable

We've helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our "Solutions" page to see the areas of your business we can help improve to see if we're a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide "Preparing Your AP Department For The Future"

Download a free copy of our guide to future proofing your accounts payable department. You'll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts